

AFFIDAVIT

I, Jamie West, having been first duly sworn, do hereby depose and state as follows:

1. I am a Special Agent with Homeland Security Investigations (HSI). HSI is a directorate within Immigration and Customs Enforcement (ICE). ICE is a subordinate component of the Department of Homeland Security (DHS) and the successor to many of the law enforcement powers of the former Immigration and Naturalization Service and the former U.S. Customs Service. I have been a Special Agent since January 2002 and I am currently assigned to HSI Derby Line, Vermont. I have investigated federal criminal violations related to technology and cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center and work relating to conducting these types of investigations. I have had discussions with other law enforcement officers, including Vermont Office of Attorney General Detective Matthew Raymond, about how people use computers to commit crimes and the law enforcement techniques that can be utilized to investigate and disrupt such activity. I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251 and 2252, and I am authorized by law to request a search warrant.
2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of Electronic Devices, described with particularity in Attachment A, and the extraction from the Electronic Devices of electronically stored information described in Attachment B.
3. The property to be searched is the contents of multiple electronic devices and data storage seized from the residence of Norman MERRILL II (32 Regina Lane, Chester, Vermont) on May 11, 2022 by Chester Police in case number 22 CH 000716, referred to hereafter as “the Electronic

Devices,” currently in the possession of the Vermont State Police Computer Crimes Unit in Waterbury, Vermont:

- a. 3 black Apple iPhones
- b. 2 Seagate 2 TB Portable Drives
- c. 1 camera with no battery
- d. 1 camera with SD card and no battery
- e. 1 camera with battery and micro SD card
- f. 1 red Apple iPhone
- g. 1 SanDisk Micro SD Ultra Card with QGeem adapter
- h. 1 SanDisk USB/USBC Thumb Drive
- i. 1 Power block camera
- j. 1 blue Amazon Kindle
- k. 1 Apple iPad with Black case
- l. 1 SanDisk 4 GB Micro SD Card
- m. 1 SanDisk Memory Stick Pro Duo
- n. 1 SanDisk Cruzer 4 GB USB with Red tip
- o. 1 128 GB Micro SD Card with Adapter
- p. 1 red Kinston 8 GB USB drive
- q. 1 green and yellow USB drive
- r. 1 black Western Digital hard drive
- s. 1 Apple iPad blue case
- t. 1 Apple Macbook in case
- u. 1 Apple Mac Mini Compact Computer

The applied-for warrant would authorize the forensic examination of the Electronic Devices and any digital storage contained within them, for the purpose of identifying electronically stored data particularly described in Attachment B.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that evidence

of crimes committed by Norman MERRILL are located in the data contained on the Electronic Devices, specifically the production and attempted production of visual depictions of minors engaged in sexually explicit conduct in violation of 18 U.S.C. § 2251(a) and (e); possession of visual depictions of minors engaging in sexually explicit conduct, in violation of 18 U.S.C.

§ 2252(a)(4)(B); and production with intent to distribute or distribution of child pornography that is an adapted or modified depiction of an identifiable minor, in violation of 18 U.S.C. § 2252A(a)(7).

5. I am familiar with the facts and circumstances of this investigation from: (a) my own personal involvement in the investigation and my personal observations; (b) my review of documents and reports, and conversations with Chester Police Detective Adam C. Woodell and Detective Sergeant Eric Jollymore of the Vermont State Police and other law enforcement officers, and (c) my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned by law enforcement during the course of the investigation. Unless otherwise noted, any statements described herein are in sum and substance, and are not intended to reflect verbatim quotations.

PROBABLE CAUSE

6. On May 7, 2022, [REDACTED] contacted the Chester Police Department (PD) to report that [REDACTED] had found Merrill's old cell phone concealed in a box in the kids' bathroom, and the camera of the phone appeared pointed at the shower. [REDACTED] was subsequently interviewed by Chester PD Officer Adam Woodell. [REDACTED] told Officer Woodell about finding the cell phone (a black iPhone), described it as being in a black/blue "shaving razor cardboard box" which had a small hole cut in it, and that the phone was connected to a black external battery charger. [REDACTED] told Officer Woodell that after she had found the hidden phone in the cardboard box, the box was later replaced with a nearly

identical box which lacked the small hole. [REDACTED] was interviewed. [REDACTED]

[REDACTED] reported that in the past she saw a suspicious device on the wall of the same bathroom, which appeared to be a smoke detector pointed at the shower, and which was later removed. [REDACTED]

[REDACTED] also witnessed Merrill photograph Minor Victim 1 discreetly while walking behind her.

7. On May 10, 2022, Chester Police obtained a state search warrant which authorized a search of Merrill's residence for black iPhones and the shaving razor cardboard box. This warrant was executed on May 11, 2022. During the search, officers located a black and blue colored Bump Patrol Aftershave cardboard box that had a small hole cut in the box. While searching for black iPhones, the agents examined the contents of an unlocked fire-resistant safe. Inside the safe, officers located suspicious electronics including two pinhole/spy cameras, which are types of surveillance cameras designed to be hidden in a location that conceals them from detection, and a USB charging block that appeared to have a lens.

8. During the officers' execution of the search warrant, Merrill was interviewed. Among other statements during the interview, Merrill denied having any electronic devices other than his cellular phone. Merrill also admitted to having put a shaving box and other items in the "kids' bathroom," claiming he had been cleaning out his son's room.

9. On May 11, 2022, Chester Police obtained a second search warrant, authorizing the seizure and search of all electronic devices within Merrill's residence. An on-scene preview of a SanDisk 128GB SD card that was seized from Merrill's residence revealed a number of video and image files indicating likely voyeurism, with videos recorded in bathrooms. A full extraction of the data from the SanDisk 128GB SD card was provided to me by VSP Det. Sgt. Jollymore. I have compared some of the videos to photographs Chester Police took of the "kids' bathroom" in Merrill's

residence, and the bathrooms appear identical.¹ I have reviewed two of these videos closely. The file name of the first video is “IMG_0113.mov”; the file name of the second video is “mmmmmm.avi”.

10. “IMG_0113.mov” begins depicting Merrill, who is wearing a Green Mountain Union High School sweatshirt. In the video, Merrill is seen placing the device in a hidden location on or very near the floor. Merrill spends a few minutes adjusting the upward angle of the camera, and ensuring it is adequately hidden from view. After approximately 26 minutes, Minor Female 1 appears in the video. Minor Female 1 is identifiable by both her face, and her last name appears on the sleeve of her sweatshirt. Minor Female 1 has been interviewed by law enforcement. As of May 2022, Minor Female 1 is under the age of 16. The video captures Minor Female 1 disrobing, and due to the angle of the video, Minor Female 1’s genitalia is observed briefly as she removes her underwear. Minor Female 1’s genitalia is also seen later in the video, as she is close to the sink in the bathroom. Minor Female 1 appears to wash her face, and after drying her face, the camera becomes obscure.

11. “mmmmmm.avi” depicts Minor Female 1 in the same bathroom, however, the video is taken at a different angle. Minor Female 1 is identifiable by her face, which is clearly visible at various points in the video. Minor Female 1 was shown a still image of this video and identified herself. The camera appears to have been placed near the sink, at approximately the level of Minor Female 1’s pubic area. The “mmmmmm.avi” video also captures Minor Female 1 disrobing and completely nude. Due to the placement of the camera, there are multiple incidents of extreme close-ups of Minor Female 1’s genitalia.

12. I examined images recovered from the SanDisk 128GB SD card seized from Merrill’s

¹ There are videos that appear to be “mirrored,” in that the bathroom is flipped as if viewed through a mirror. The other characteristics of the bathroom (including the color and pattern of the shower curtain and general layout) match the “kids’ bathroom” in Merrill’s residence.

residence, and located multiple image files that appear to be “screen captures” taken from the mmmmmm.avi video. That is, in viewing the video mmmmmm.avi, I saw the same depiction in the video as in the still image. Some of these still images depict Minor Female 1 nude, and they only depict Minor Female 1 from her chest to her upper thigh, with her genitals and pubic area clearly visible.

13. I also examined other images recovered from the SanDisk 128GB SD card seized from Merrill’s residence, and located what appeared to be “screen shots” of a social media profile for an identifiable teenager in the Chester area: Minor Female 2. Law enforcement has spoken with Minor Female 2’s parent. As of May 2022, Minor Female 2 is under the age of 16. I also located an image file of adult pornography that depicted an adult male having anal intercourse with an adult female. However, the face of the adult female had been altered, and the face of Minor Female 2 appears to have been superimposed over the adult female’s face. That is, the face of an identifiable minor was placed into a visual depiction of sexually explicit conduct in a manner that the minor appears to be engaging in the sexually explicit conduct.

14. The SanDisk 128 GB SD card was manufactured in China.

15. The Electronic Devices which were seized by Chester Police were all subsequently provided to the Vermont State Police for full forensic examinations. The Electronic Devices are currently in the custody of the Vermont State Police.

16. Merrill was the only adult residing in his residence at the time the search warrant was executed. His current wife, who lives out of state, visited him at the residence approximately one weekend a month. She was at the residence on May 7, 2022. Merrill’s adult son was also at the residence that weekend, but according to [REDACTED], he did not arrive until the day after she discovered the cell phone concealed in a box. [REDACTED] who found the cell phone in the

box [REDACTED].

17. On May 19, 2022, the federal grand jury sitting in Burlington, Vermont returned a three-count indictment charging Merrill with violations of 18 U.S.C. § 2251(a) (production of child pornography), 18 U.S.C. § 2251(a) & 2251(e) (attempted production of child pornography), and 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography).

18. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Cellular telephone: A cellular telephone (or mobile telephone, or wireless telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A cellular telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, electronic devices offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Electronic devices may also include global positioning system (“GPS”) technology for determining the location of the device.

b. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication Device and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and

presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device. PDAs also often contain digital cameras.

c. Smart Phone: Smart phone is a term typically used to refer to a cellular telephone that has combined the capabilities of a typical cellular telephone and a typical PDA.

d. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

e. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation Devices can give a user driving or walking directions to another location. These Devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some

computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between Device on the Internet often cross state and international borders, even when the Device communicating with each other are in the same state.

23. Based on my training and experience, I know the black iPhones and red iPhone are Smartphones with all of the features outlined above. The Mac Mini and tablet computers do not function as cellular devices by design, but applications can be installed on each of those devices that allow them to make telephone calls and perform other functions of a traditional cellphone. The remaining items are data storage items or could contain unique device information (model number and serial number).

24. In addition, I submit that there is probable cause to believe records may be stored on the Electronic Devices for at least the following reasons:

a. Based on my knowledge, training, experience and discussions with other law enforcement officers, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer or smart phone, the data contained in the file does not actually disappear; rather, that data remains on the device’s storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by and active file – for long periods of time before they are overwritten. In addition, a device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media – in particular, a device’s internal hard drives – contain electronic evidence of how a computer has been used,

what it has been used for, and who has used it (user attribution). To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into temporary Internet directory or “cache.”

25. As further described in Attachment B, this application seeks permission to locate not only digital files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the Electronic Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe this forensic electronic evidence will be on the Electronic Devices for the following reasons:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage Device or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created, and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry

information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus spyware and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner’s motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a “wiping” program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a cellular telephone works can, after examining this forensic evidence in its proper context, draw conclusions about how a cellular telephone was used, the purpose of its use, who used it, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

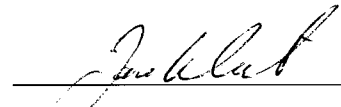
e. Further, in finding evidence of how a cellular telephone was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

26. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION


27. Based on the foregoing, I submit probable cause exists to search the Electronic Devices, more specifically described in Attachment A, for the evidence delineated in Attachment B.

Dated at Burlington, in the District of Vermont, this 26th day of May, 2022.



SA Jamie West
Homeland Security Investigations

Sworn to and subscribed before me this 26th day of May, 2022.



HON. KEVIN J. DOYLE
United States Magistrate Judge